



(43) 國際公開日
2005 年 5 月 12 日 (12.05.2005)

PCT

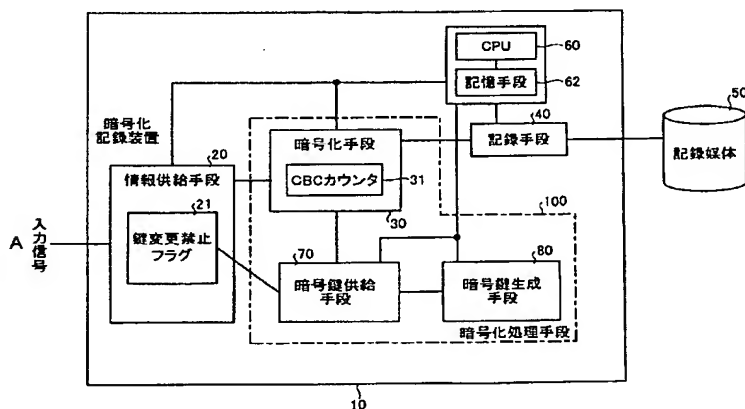
(10) 国際公開番号
WO 2005/043806 A1

- | | | |
|--------------------------------|----------------------------------|---|
| (51) 国際特許分類 ⁷ : | H04L 9/14, 9/16 | (71) 出願人 (米国を除く全ての指定国について): パイオニア株式会社 (PIONEER CORPORATION) [JP/JP]; 〒1538654 東京都目黒区目黒 1 丁目 4 番 1 号 Tokyo (JP). |
| (21) 国際出願番号: | PCT/JP2004/016149 | |
| (22) 国際出願日: | 2004 年 10 月 29 日 (29.10.2004) | (72) 発明者; および |
| (25) 国際出願の言語: | 日本語 | (75) 発明者/出願人 (米国についてのみ): 多田 謙一郎 (TADA, Kenichiro) [JP/JP]. |
| (26) 国際公開の言語: | 日本語 | (74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1000013 東京都千代田区麹が関三丁目 2 番 6 号 東京倶楽部ビルディング 酒井国際特許事務所 Tokyo (JP). |
| (30) 優先権データ:
特願 2003-372215 | 2003 年 10 月 31 日 (31.10.2003) JP | (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, |

〔統葉有〕

(54) Title: ENCRYPTION/RECORDING DEVICE AND METHOD

(54) 発明の名称: 暗号化記録装置および方法



- A...INPUT SIGNAL
10...ENCRYPTION/RECORDING DEVICE
20...INFORMATION SUPPLY MEANS
21...KEY MODIFICATION INHIBIT FLAG
30...ENCRYPTION MEANS
31...CBC COUNTER
70...ENCRYPTION KEY SUPPLY MEANS
62...STORAGE MEANS
40...RECORDING MEDIUM
80...ENCRYPTION KEY GENERATION MEANS
100...ENCRYPTION PROCESSING MEANS
50...RECORDING MEDIUM

(57) Abstract: It is possible to obtain a smooth video display not interrupted by a decryption key modification processing when performing a special reproduction such as fast-feed reproduction and search. There is provided an encryption/recording device including: information supply means (20) supplied with encoded data containing an encoding unit having an in-frame encrypted image (I picture) and other encoded image (P picture, B picture); encryption processing means (100) for encrypting the encoded data from the information supply means (20) for each predetermined encryption unit and modifying an encryption key for every one or more encryption units; and recording means (40) for recording the encrypted data. When the encryption key modification timing is in the middle of encryption of the in-frame encoded image (I picture), the encryption processing means (100) delays the key modification timing so that the encryption key modification timing is not in the middle of the in-frame encoded image (I picture).

(57) 要約: 早送り再生、サーチ等の特殊再生を行う際に、復号鍵の変更処理が介入しないスムーズな映像表示をなし得ること。フレーム内符号化画像(1ピクチャ)

〔統葉有〕



BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE,

IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

およびその他の符号化画像 (Pピクチャ, Bピクチャ) を有する符号化単位を含む符号化データが入力される情報供給手段 (20) と、情報供給手段 (20) からの符号化データを所定の暗号化単位毎に暗号化するとともに、一又は複数の暗号化単位毎に暗号鍵を変更する暗号化処理手段 (100) と、暗号化されたデータを記録する記録手段 (40) とを備えた暗号化記録装置において、暗号化処理手段 (100) は、暗号鍵変更タイミングがフレーム内符号化画像 (Iピクチャ) を暗号化する途中となる場合は、暗号鍵変更タイミングがフレーム内符号化画像 (Iピクチャ) の途中とならないよう鍵変更タイミングを遅延させる。